EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L13	6	(US-20040025032-$ or US-20010053220-$).did. or (US-5452358-$ or US-6275586-$ or US-6654884-$ or US-6295606-$). did.	US-PGPUB; USPAT	OR	OFF	2006/05/03 09:13
L14	258	(380/42).CCLS.	US-PGPUB; USPAT; EPO	OR	OFF	2006/05/03 09:13
L15	31	(380/207).CCLS.	US-PGPUB; USPAT; EPO	OR	OFF	2006/05/03 09:13
L16	1076	(380/28).CCLS.	US-PGPUB; USPAT; EPO	OR	OFF	2006/05/03 09:13
L17	3479	DPA	US-PGPUB; USPAT	OR	OFF	2006/05/03 09:13
L18	185	Differential adj Power adj Analysis	US-PGPUB; USPAT	OR	OFF	2006/05/03 09:13
L19	3518	((Differential adj Power adj Analysis) DPA)	US-PGPUB; USPAT	OR	OFF	2006/05/03 09:13
L20	1	("5452358").PN.	US-PGPUB; USPAT	OR	OFF	2006/05/03 09:13
L21	21	("4233577" | "4890324" | "5351299").PN. OR ("5452358"). URPN.	US-PGPUB; USPAT; USOCR	OR	OFF	2006/05/03 09:13
L22	49	("6125182" "6128386" "6804354" "5937066" "5479513" "5438622" "6393125" "5677956" "6760440" "6031911" "5966450" "5970148" "6205249" "5799090" "6044388" "6061703" "6061703" "6104810" "6324287" "5717760" "6763363" "5796830" "5003597" "5258936" "6052469" "5452358" "6021203" "6052466" "6088456" "6266413" "6269164" "6415032" "6445794" "6490354" "6870930" "6425081" "6769063" "5454039" "5675652" "5835597" "5301247" "5345508" "5444781" "5995625" "6049874" "6549622" "6917218" "6182216" "6199162" "6578150").pn.	US-PGPUB; USPAT	OR	OFF	2006/05/03 09:13

EAST Search History

L23	48	("6751319" "5363448" RE36181 "5377270" RE36752 "6339824" "6178244" "5751811" "4897876" "5841872" "5963104" "6278802" "6069954" "6278783" "6578061" "6850960" "6859818" "6081598" "5940514" "6381072" "5768390" "5475826" "5675653" "5694569" "6038665" "6061449" "6061449" "6526145" "6870929" "5956404" "5365589" "5604801" "5481613" "5535277" "5588060" "5600720" "5633933" "5703952" "5832090" "5995623" "6002769" "6199049" "4797920" "4799061" "4924515" "4934846" "5196840" "5351293" "5455862").pn.	US-PGPUB; USPAT	OR	OFF	2006/05/03 09:13
L24	4	Rijndael and L17	US-PGPUB; USPAT	OR	OFF	2006/05/03 09:13
L25	21	(Differential adj Power adj Analysis) and ((lookup or look-up) with table)	US-PGPUB; USPAT	OR	OFF	2006/05/03 09:13
L26	78	(380/263).CCLS.	US-PGPUB; USPAT; EPO	OR	OFF	2006/05/03 09:13
L27	224	((Differential adj Power adj Analysis) DPA) and ((plurality multiple set$1) same mask$4)	US-PGPUB; USPAT	OR	OFF	2006/05/03 09:13
L28	7	(L14 L15 L16 L26) and L27	US-PGPUB; USPAT	OR	OFF	2006/05/03 09:13
L29	284	Rijndael	US-PGPUB; USPAT	OR	OFF	2006/05/03 09:13
L30	224	((Differential adj Power adj Analysis) DPA) and ((plurality multiple set$1) same mask$4)	US-PGPUB; USPAT	OR	OFF	2006/05/03 09:13
L31	12	((Differential adj Power adj Analysis) DPA) same ((plurality multiple set$1) same mask$4)	US-PGPUB; USPAT	OR	OFF	2006/05/03 09:13
L32	773	((Differential adj Power adj Analysis) DPA) same (table matrix set)	US-PGPUB; USPAT	OR	OFF	2006/05/03 09:13
L33	235	((Differential adj Power adj Analysis) DPA) with (table matrix set)	US-PGPUB; USPAT	OR	OFF	2006/05/03 09:13
L34	376	(713/194).CCLS.	US-PGPUB; USPAT; EPO	OR	OFF	2006/05/03 09:13
L35	938	(713/189).CCLS.	US-PGPUB; USPAT; EPO	OR	OFF	2006/05/03 09:13

EAST Search History

L36	144	(726/34).CCLS.	US-PGPUB; USPAT; EPO	OR	OFF	2006/05/03 09:13
L37	60	(326/8).CCLS.	US-PGPUB; USPAT; EPO	OR	OFF	2006/05/03 09:13
L38	43	(726/36).CCLS.	US-PGPUB; USPAT; EPO	OR	OFF	2006/05/03 09:13
L39	68	(L14 L15 L16 L26 L34 L35 L37 L38 L36) and ((Differential adj Power adj Analysis) DPA)	US-PGPUB; USPAT; EPO	OR	OFF	2006/05/03 09:13
L40	43	(726/36).CCLS.	US-PGPUB; USPAT; EPO	OR	OFF	2006/05/03 09:13
L41	60	(326/8).CCLS.	US-PGPUB; USPAT; EPO	OR	OFF	2006/05/03 09:13

Key: IEEE JNL = IEEE Journal or Magazine, IEE JNL = IEE Journal or Magazine, IEEE CNF = IEEE Conference, II CNF = IEE Conference, IEEE STD = IEEE Standard

1. **Power analysis attacks and algorithmic approaches to their countermeasures for Koblitz curve cryptosystems**
   Hasan, M.A.;
   Computers, IEEE Transactions on
   Volume 50, Issue 10, Oct. 2001 Page(s):1071 - 1083
   IEEE JNL

2. **Energy-aware design techniques for differential power analysis protection**
   Benini, L.; Omerbegovic, E.; Macii, A.; Poncino, M.; Macii, E.; Pro, F.;
   Design Automation Conference, 2003. Proceedings
   2-6 June 2003 Page(s):36 - 41
   IEEE CNF

3. **Smart cards inside**
   Gammel, B.M.; Ruping, S.J.;
   Solid-State Device Research Conference, 2005. ESSDERC 2005. Proceedings of 35th European
   12-16 Sept. 2005 Page(s):69 - 74
   IEEE CNF

4. **Smart cards inside**
   Gammel, B.M.; Ruping, J.;
   Solid-State Circuits Conference, 2005. ESSCIRC 2005. Proceedings of the 31st European
   12-16 Sept. 2005 Page(s):69 - 74
   IEEE CNF

5. **Design of an RSA module against power analysis attacks**
   Jiang Huiping; Mao Zhigang;
   ASIC, 2003. Proceedings. 5th International Conference on
   Volume 2, 21-24 Oct. 2003 Page(s):1308 - 1311 Vol.2
   IEEE CNF

6. **Masking the energy behaviour of encryption algorithms**
   Saputra, H.; Vijaykrishnan, N.; Kandemir, M.; Irwin, M.J.; Brooks, R.;
   Computers and Digital Techniques, IEE Proceedings-
   Volume 150, Issue 5, 22 Sept. 2003 Page(s):274-84
   IEE JNL

7. **A countermeasure for EM attack of a wireless PDA**
   Gebotys, C.H.; Tiu, C.C.; Chen, X.;
   Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference on
   Volume 1, 4-6 April 2005 Page(s):544 - 549 Vol. 1
   IEEE CNF

8. **An overview of power analysis attacks against field programmable gate arrays**
   Standaert, O.-X.; Peeters, E.; Rouvroy, G.; Quisquater, J.-J.;
   Proceedings of the IEEE
   Volume 94, Issue 2, Feb. 2006 Page(s):383 - 394
   IEEE JNL

9. **Masking the energy behavior of DES encryption [smart cards]**
Saputra, H.; Vijaykrishnan, N.; Kandemir, M.; Irwin, M.J.; Brooks, R.; Kim, S.; Zhang, W.;
Design, Automation and Test in Europe Conference and Exhibition, 2003
2003 Page(s):84 - 89
IEEE CNF

10. **AES-Based Security Coprocessor IC in 0.18-$muhbox m$CMOS With Resistance to Differential Power Analysis Side-Channel Attacks**
Hwang, D.D.; Tiri, K.; Hodjat, A.; Lai, B.-C.; Yang, S.; Schaumont, P.; Verbauwhede, I.;
Solid-State Circuits, IEEE Journal of
Volume 41, Issue 4, April 2006 Page(s):781 - 792
IEEE JNL

11. **All-digital PLL and transmitter for mobile phones**
Staszewski, R.B.; Wallberg, J.L.; Rezeq, S.; Chih-Ming Hung; Eliezer, O.E.; Vemulapalli, S.K.; Fernando, C.; Maggi K.; Staszewski, R.; Barton, N.; Meng-Chang Lee; Cruise, P.; Entezari, M.; Muhammad, K.; Leipold, D.;
Solid-State Circuits, IEEE Journal of
Volume 40, Issue 12, Dec. 2005 Page(s):2469 - 2482
IEEE JNL

12. **On the masking countermeasure and higher-order power analysis attacks**
Standaert, F.-X.; Peeters, E.; Quisquater, J.-J.;
Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference on
Volume 1, 4-6 April 2005 Page(s):562 - 567 Vol. 1
IEEE CNF

13. **Towards an AES crypto-chip resistant to differential power analysis**
Pramstaller, N.; Gurkaynak, F.K.; Haene, S.; Kaeslin, H.; Felber, N.; Fichtner, W.;
Solid-State Circuits Conference, 2004. ESSCIRC 2004. Proceeding of the 30th European
21-23 Sept. 2004 Page(s):307 - 310
IEEE CNF

14. **Area, throughput and security considerations for AES crypto-ASICs**
Gurkaynak, F.K.; Felber, N.; Kaeslin, H.; Fichtner, W.;
Research in Microelectronics and Electronics, 2005 PhD
Volume 2, 25-28 July 2005 Page(s):218 - 221
IEEE CNF

15. **Partitioning attacks: or how to rapidly clone some GSM cards**
Rao, J.R.; Rohatgi, P.; Scherzer, H.; Tinguely, S.;
Security and Privacy, 2002. Proceedings. 2002 IEEE Symposium on
2002 Page(s):31 - 41
IEEE CNF

16. **A countermeasure against differential power analysis based on random delay insertion**
Bucci, M.; Luzzi, R.; Guglielmo, M.; Trifiletti, A.;
Circuits and Systems, 2005. ISCAS 2005. IEEE International Symposium on
23-26 May 2005 Page(s):3547 - 3550 Vol. 4
IEEE CNF

17. **On active camera control and camera motion recovery with foveate wavelet transform**
Wei, J.; Li, Z.-N.;
Pattern Analysis and Machine Intelligence, IEEE Transactions on
Volume 23, Issue 8, Aug. 2001 Page(s):896 - 903
IEEE JNL

18. **An on-chip signal suppression countermeasure to power analysis attacks**
Ratanpal, G.B.; Williams, R.D.; Blalock, T.N.;
Dependable and Secure Computing, IEEE Transactions on
Volume 1, Issue 3, July-Sep 2004 Page(s):179 - 189
IEEE JNL

19. **Charge recycling sense amplifier based logic: securing low power security ICs against DPA [differential power analysis]**
Tiri, K.; Verbauwhede, I.;
Solid-State Circuits Conference, 2004. ESSCIRC 2004. Proceeding of the 30th European
21-23 Sept. 2004 Page(s):179 - 182
IEEE CNF

20. **Are we really ready for the breakthrough? [morphware]**
Hartenstein, R.;
Parallel and Distributed Processing Symposium, 2003. Proceedings. International
22-26 April 2003 Page(s):7 pp.
IEEE CNF

21. **All-digital PLL and GSM/EDGE transmitter in 90nm CMOS**
Staszewski, R.B.; Wallberg, J.; Rezeq, S.; Chih-Ming Hung; Eliezer, O.; Vemulapalli, S.; Fernando, C.; Maggio, K.; Staszewski, R.; Barton, N.; Meng-Chang Lee; Cruise, P.; Entezari, M.; Muhammad, K.; Leipold, D.;
Solid-State Circuits Conference, 2005. Digest of Technical Papers. ISSCC. 2005 IEEE International
6-10 Feb. 2005 Page(s):316 - 600 Vol. 1
IEEE CNF

22. **Instruction stream mutation for non-deterministic processors**
Irwin, J.; Page, D.; Smart, N.P.;
Application-Specific Systems, Architectures and Processors, 2002. Proceedings. The IEEE International Conferenc on
17-19 July 2002 Page(s):286 - 295
IEEE CNF

23. **Power attack resistant cryptosystem design: a dynamic voltage and frequency switching approach**
Shengqi Yang; Wolf, W.; Vijaykrishnan, N.; Serpanos, D.N.; Yuan Xie;
Design, Automation and Test in Europe, 2005. Proceedings
2005 Page(s):64 - 69 Vol. 3
IEEE CNF

24. **IT security project: implementation of the Advanced Encryption Standard (AES) on a smart card**
Schramm, K.; Paar, C.;
Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference on
Volume 1, 2004 Page(s):176 - 180 Vol.1
IEEE CNF

25. **Design and implementation of high-speed symmetric crossbar schedulers**
Hurt, J.; May, A.; Zhu, X.; Lin, B.;
Communications, 1999. ICC '99. 1999 IEEE International Conference on
Volume 3, 6-10 June 1999 Page(s):1478 - 1483 vol.3
IEEE CNF